RFC-0008 Continuous Reporting Standard

Friday, May 9th, 2025

Background

OMB Circular A-130: Managing Information as a Strategic Resource defines continuous monitoring as *“maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.”*

The FedRAMP Authorization Act (44 USC § 3609 (a) (1)) directs the Administrator of the General Services Administration to *“... develop, coordinate, and implement a process to support agency review, reuse, and standardization, where appropriate, of security assessments of cloud computing products and services, including, as appropriate, oversight of continuous monitoring of cloud computing products and services...”* This responsibility is delegated to the FedRAMP Director.

Introduction

This FedRAMP standard establishes an updated continuous monitoring reporting process for FedRAMP authorized cloud service providers that requires cloud service providers to maintain direct relationships with their customers for reporting purposes and reduce the burden for continuous monitoring by agencies. Agencies must follow OMB policy and NIST standards when adopting FedRAMP authorized cloud services, including maintaining an ongoing awareness of the security posture of services they use. Providers must ensure such information is available directly to agencies and regularly review it with all participating agencies.

To ensure maximum reusability across agencies and encourage private sector innovation, continuous monitoring reporting must follow an objective data-driven approach that makes key security metrics easy for providers to collect and easy for agencies to monitor. Reporting should focus on information agencies need to know and will benefit from reviewing. The entire continuous monitoring and reporting process should encourage and empower engineering and security teams at providers to focus on maintaining and improving the security of their systems.

This updated standard creates a new Continuous Reporting Standard that replaces some parts of previous FedRAMP guidance related to reporting on continuous monitoring activities for all FedRAMP authorizations and certifications, including the current Rev 5 Agency Authorization process and FedRAMP 20x. Best practices and technical assistance to help stakeholders follow this standard will be provided separately.

This standard does not change the continuous monitoring requirements identified in a provider's security plan; it only changes the reporting requirements. Additional information on how these requirements will change overall and align to emerging standards such as the Significant Change Notification Standard will be provided prior to final formalization of this standard.

No action will be required of any cloud service provider without supporting guidance based on this FedRAMP Standard.

Continuous Reporting

The FedRAMP Continuous Reporting Standard establishes requirements for continuous reporting that cloud service providers MUST follow to maintain FedRAMP authorization.

At least the following Key Security Metrics MUST be included in continuous monitoring reports:

A. **Unmitigated Vulnerabilities** - A list of unmitigated vulnerabilities or vulnerability groupings, broken down by risk rating, including at least the following information:

   a. Total number of unmitigated items
   b. Common Vulnerabilities and Exposures (CVE) ID, other unique ID if CVE is unavailable, or N/A
   c. Provider’s unique tracking identifier for this occurrence
   d. Component or Services impacted
   e. Original FedRAMP remediation window end date
   f. Known Exploited Vulnerability status
   g. Remediation and/or mitigation plans, including dates

B. **Mitigated Vulnerabilities** - A list of mitigated vulnerabilities or vulnerability groups, broken down by estimated risk rating after mitigation, including at least the following information:

   a. Total number of mitigated items
   b. Common Vulnerabilities and Exposures (CVE) ID, other unique ID if CVE is unavailable, or N/A
   c. Provider’s unique tracking identifier for this occurrence
   d. Component or Services impacted
   e. Original risk rating prior to mitigation
   f. Explanation of mitigation measures
   g. Date mitigation took effect
   h. Original FedRAMP remediation window end date
   i. Known Exploited Vulnerability status
   j. Remediation plan, including dates

C. **Incidents** - Information about any incident-related activities in the past reporting period or past 30 days (whichever is longer)

D. **Significant Change Notifications** - Information about any Significant Change Notifications in the past reporting period or past 30 calendar days (whichever is longer)

E. **Upcoming Milestones** - Information about any upcoming planned service milestones and third-party assessment activities within the next 60 calendar days that are not included in Significant Change Notifications

F. **Overall Scan Coverage** - Overall numbers and percentage of distinct component configurations covered by the service's security scanning activities

G. **Detailed Component Scan Coverage** - Numbers and percentage of components covered by the services's security scanning activities grouped by distinct component type and scan type

Application of the Continuous Reporting Standard

1. Providers MUST make Key Security Metrics available to agencies and FedRAMP in similar human-readable and compatible machine-readable formats. These formats SHOULD follow FedRAMP best practices and technical assistance to ensure maximum reusability.

2. Providers MUST update Key Security Metrics at least monthly.

3. Providers MUST keep Key Security Metrics available to agencies and FedRAMP for 24 months after initial reporting.

4. Providers SHOULD update Key Security Metrics one week before monthly monitoring meetings to ensure information is timely and agencies and FedRAMP have the opportunity to review in advance.

5. Providers SHOULD make Key Security Metrics available within their standard customer portals, protected with appropriate controls to ensure agencies and FedRAMP can make this information available to their information

security staff.

6. Providers SHOULD mitigate vulnerability risk as quickly as possible. Providers SHOULD adjust vulnerability severity based on documented mitigation.

7. Providers, third-party assessment organizations, agencies, and FedRAMP SHOULD consider mitigated vulnerabilities at their mitigated risk rating. Providers MAY carry mitigated vulnerabilities beyond FedRAMP remediation windows for the original risk rating without penalty but MUST remediate such vulnerabilities once it is reasonable to do so.

8. Providers SHOULD NOT include validated false positives in security reporting to agencies and FedRAMP. Providers MUST maintain documented evidence for determinations of false positives for the duration of their existence.

9. Providers MAY make Key Security Metrics available to other customers or the public if they determine doing so will not have a likely impact on the confidentiality, integrity, or availability of federal information.

10. Providers MAY provide additional security relevant metrics in their reporting as they deem appropriate for sharing with agencies and FedRAMP.

11. All parties SHOULD follow FedRAMP’s best practices and technical assistance on continuous reporting where applicable.

Exceptions to the Continuous Monitoring Reporting Requirements

Providers MAY be required to provide additional metrics beyond those identified above as a condition of a formal FedRAMP Corrective Action Plan or other agreements with federal agencies.